PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-088279
(43)Date of publication of application : 18.03.2004

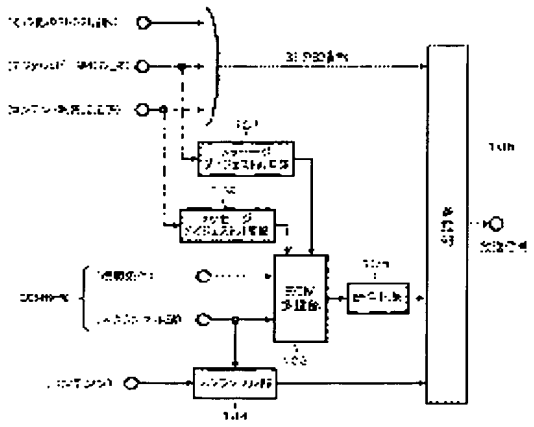
(51)Int.CI. H04L 9/32
G09C 1/00
H04H 1/00
H04J 3/00
H04L 9/08
H04N 7/08
H04N 7/081
H04N 7/167

(21)Application number : 2002-244570
(22)Date of filing : 26.08.2002

(71)Applicant : TOSHIBA CORP
(72)Inventor : OI SHINICHI

(54) BROADCAST TRANSMISSION METHOD AND RECEIVER

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent piracy due to falsified copyright protection information.
SOLUTION: In order to prevent falsification of a digital copy control descriptor and a content utilization descriptor being the copyright protection information, a transmitter side calculates falsification detection data of each descriptor, attaches the data to an ECM and transmits the resulting ECM. A receiver side decides presence / absence of falsification on the basis of received digital copy control descriptor, content utilization descriptor and falsification detection data in the ECM. In the case of decision of the presence of falsification, control of disabled viewing or the like is executed to suppress the falsification thereby protecting the copyright.



LEGAL STATUS

[Date of request for examination] 26.08.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-88279
(P2004-88279A)
(43)公開日　平成16年3月18日(2004.3.18)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/32	H04L	9/00	675A	5C063
G09C	1/00	G09C	1/00	640D	5C064
H04H	1/00	H04H	1/00	B	5J104
H04J	3/00	H04H	1/00	F	5K028
H04L	9/08	H04J	3/00	A	

審査請求 未請求　請求項の数 6　OL　（全 11 頁）　最終頁に続く

(21)出願番号　特願2002-244570(P2002-244570)
(22)出願日　平成14年8月26日(2002.8.26)

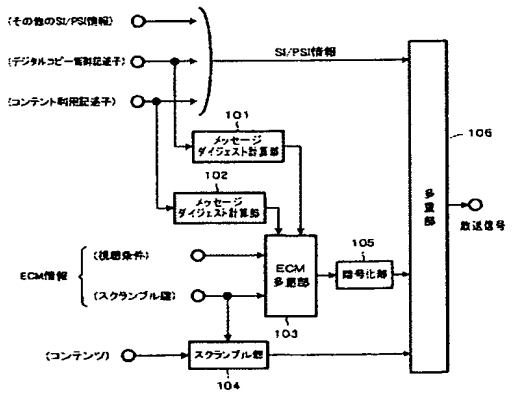
(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100083161
弁理士　外川　英明
(72)発明者　大井　伸一
東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内

Fターム(参考)　5C063 AA01 AB03 AB07 AC01 AC05
AC10 CA23 CA36 DA07 DA13
DB10
5C064 BA01 BB02 BC06 BC17 BC18
BC22 BC25 BD02 BD08 BD09
CA14 CB01 CC02 CC04

最終頁に続く

(54)【発明の名称】放送送信方法および受信装置

(57)【要約】
【課題】著作権保護情報の改ざんによる著作権侵害を防止する。
【解決手段】著作権保護用の情報であるデジタルコピー制御記述子およびコンテント利用記述子の改ざんを防止するために、送信側で各記述子の改ざん検出データを計算し、ＥＣＭに入れて伝送する。受信側で受信したデジタルコピー制御記述子およびコンテント利用記述子とＥＣＭ内の改ざん検出データから、改ざんの有無を判定する。改ざんと判定された場合は視聴不可等の制御を行い、改ざんの抑止することで著作権保護が可能となる。



1

【特許請求の範囲】
【請求項１】
デジタル放送に使用される番組配列情報の一部とされる著作権保護方式の保護情報であるデジタルコピー制御記述子およびコンテント利用記述子のうち、少なくとも一方の前記記述子をスクランブルされた番組とともに送信する放送送信方法において、
送信される前記記述子が伝送路における改ざんの有無を受信装置側で検出するために前記記述子から改ざん検出データを生成し、全受信装置共通の番組のスクランブルを解くための鍵や番組の属性情報を参照する番組情報（ＥＣＭ）に多重して暗号化させた情報を、前記スクランブルされた番組とともに多重させて伝送することを特徴とする放送送信方法。
【請求項２】
受信側で送信された前記記述子に改ざん有りと検出された場合に、受信側が動作すべき制御方法が規定された改ざん検出時の制御モード情報をさらに多重させて伝送したことを特徴とする請求項１記載の放送送信方法。
【請求項３】
請求項１に基づいて多重して送信される前記記述子および番組を受信する放送受信装置において、
送信される前記記述子の伝送路における改ざんの有無を検出し、改ざんがあったと判定された場合は、デスクランブルを不可とする手段を具備むしたことを特徴とする放送受信装置。
【請求項４】
請求項１に基づいて多重して送信される前記記述子および番組を受信する放送受信装置において、
前記番組のスクランブルを解くデスクランブル手段と、受信信号に含まれる非暗号化の前記記述子および受信信号に含まれる全受信装置共通の番組のスクランブルを解くための鍵や番組の属性情報を参照する番組情報（ＥＣＭ）とともに暗号化された前記改ざん検出データを計算した結果とに基づき改ざんを判定する手段と、
前記手段により、改ざんがあったと判定された場合は、前記デスクランブル手段によるデスクランブルを不可とする制御を行う手段とからなることを特徴とする放送受信装置。
【請求項５】
請求項２に基づいて多重して送信される前記記述子および番組および改ざん検出時の制御モード情報を受信する放送受信装置において、
前記番組のスクランブルを解くデスクランブル手段と、受信信号に含まれる非暗号化の前記記述子および受信信号に含まれる全受信装置共通の番組のスクランブルを解くための鍵や番組の属性情報を参照する番組情報（ＥＣＭ）とともに暗号化された前記改ざん検出データを計算した結果とに基づき改ざんを判定する手段と、
前記手段により、改ざんがあったと判定された場合は、

2

改ざん検出時の制御モード情報に従い、受信状態を制御する手段とを具備することを特徴とする放送受信装置。
【請求項６】
前記ＥＣＭからスクランブルされた前記番組をデスクランブルするためのスクランブル鍵を取り出すＥＣＭ処理手段、前記改ざん検出データを計算する手段、前記改ざんを判定する手段とを少なくともＩＣカード内で処理するものとし、前記デジタルコピー制御記述子もしくはコンテント利用記述子に改ざんがあった場合には、前記ＩＣカードから前記スクランブル鍵を出力しないようにしたことを特徴とする請求項４または５記載の放送受信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
この発明は、著作権保護方式に対応した放送送信方法および受信装置に関する。
【０００２】
【従来の技術】
ＡＲＩＢ（社団法人電波産業会）等で規格化検討中の「著作権保護方式」では、番組提供者の権利を保護する観点から、スクランブルを利用し、番組の権利保護が可能な受信機のみが復調できるようにしたことにより、放送された番組の不正な複製を防止することを可能にしている。
【０００３】
具体的には、デジタル放送用受信機等における番組の権利保護を、次の（１）～（３）に記載したように実現している。
（１）　番組の複製可能な回数等の番組の利用条件を、番組とともに放送波で伝送する。
（２）　放送の送り手側は番組等をスクランブルする鍵を管理し、権利保護情報に示す利用条件に従って動作をする受信機に対してその鍵を付与する。
（３）　受信機から外部接続機器に番組を出力できるのは、その外部接続機器も権利保護情報に示す番組の使用条件に従う動作をするものである場合に限る。その際、権利保護情報も付加して出力する。
【０００４】
ここで、番組の複製可能な回数等の番組の利用条件は、デジタル放送に使用される番組配列情報（ＳＩ（Ｓｅｒｖｉｃｅ　Ｉｎｆｏｒｍａｔｉｏｎ）、ＰＳＩ（Ｐｒｏｇｒａｍ　Ｓｐｅｃｉｆｉｃ　Ｉｎｆｏｒｍａｔｉｏｎ））の一部として既に定義もしくは追加定義されるもので、以下の２つの記述子がそれである。
【０００５】
（１）　デジタルコピー制御記述子
既に有料放送のための権利保護情報としてＡＲＩＢ標準規格ＡＲＩＢ　ＳＴＤ－Ｂ１０「デジタル放送に使用する番組配列情報」に定められている。制約条件なしにコ

ピー可、１世代のみコピー可（受信した放送信号を１回のみ記録できる）、コピー禁止の３状態を指定可能である。

【０００６】

（２）　コンテント利用記述子

番組配列情報に新たに導入された権利保護情報であり、コピー禁止の番組に対し、一時的な蓄積の可／不可の指定と、一時的な蓄積時間の指定（１．５時間、３時間、・・・・・・、１週間、制限無し）が可能となっているほか、受信機からデジタルで信号を出力する場合に、暗号化等により出力データを保護するかどうか指定するという「出力保護ビット」の指定も可能となっている。

【０００７】

しかしながら、規格化検討中の「著作権保護方式」におけるデジタルコピー制御記述子とコンテント利用記述子は、非暗号状態で伝送することを前提として規格化が進んでいる。受信機に入力される前段で上記２つの記述子が改ざんされた場合には、権利保護情報に示す利用条件に従って動作する正規の受信機であっても、改ざんされた記述子の内容に従って動作してしまう。このように今の規格では、不正に対し弱いという欠点がある。

【０００８】

【発明が解決しようとする課題】

上記したように、規格化検討中の「著作権保護方式」では、改ざんされた記述子の内容に従って動作してしまうことから、このように今の規格では不正に対し弱い、という問題がある。

【０００９】

この発明の目的は、著作権保護情報に改ざんがあったかどうかで視聴不可の制御を行い著作権保護を図ることにある。

【００１０】

【課題を解決するための手段】

上記した課題を解決するために、この発明では、著作権保護情報であるデジタルコピー制御記述子、コンテント利用記述子の改ざんを防止するために、送信側で保護情報であるデジタルコピー制御記述子および／またはコンテント利用記述子の改ざん検出データを計算し、番組情報であるＥＣＭに入れて伝送する。受信側では、受信したデジタルコピー制御記述子、コンテント利用記述子から改ざん検出データを計算し、ＥＣＭ内の改ざん検出データと比較し、改ざんされたかどうかを判定する。

【００１１】

上記した手段によれば、著作権保護用の情報であるデジタルコピー制御記述子、コンテント利用記述子に改ざんがあるかどうかを検出し、改ざんがあった場合は視聴不可等の制御を行い、改ざんの抑止することで著作権保護が可能となる。

【００１２】

【発明の実施の形態】

以下、この発明の実施の形態について、図面を参照しながら詳細に説明する。図１は、この発明に係る放送側について説明するためのブロック図であり、個別の視聴契約情報であるＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｍａｎａｇｅｍｅｎｔ　Ｍｅｓｓａｇｅ）の生成と多重ブロックやこの発明に直接に関係のないブロックは省略してある。

【００１３】

図１において、番組情報配列ＳＩ，ＳＰＩの情報の一部として位置付けされる著作権保護方式用の情報であるデジタルコピー制御記述子および／またはコンテント利用記述子は、これ以外の番組配列情報ＳＩ、ＰＳＩとともに多重部１０６にて放送信号に多重され放送されるほか、デジタルコピー制御記述子はメッセージダイジェスト計算部１０１にて、コンテント利用記述子はメッセージダイジェスト計算部１０２にて改ざん検出データであるメッセージダイジェストの計算をそれぞれ行い、全受信装置共通のＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ）とともにＥＣＭ多重部１０３へ入力される。

【００１４】

ここで、ＥＣＭは、放送が有料か無料かを表す属性情報のほか、有料放送である場合には各受信機が予め放送局から送信され受信し保持しているＥＭＭと比較し、視聴が可能かどうかを判定するために使用する情報であり、すなわち番組の視聴条件を示す番組情報である。

【００１５】

また、改ざん検出データであるメッセージダイジェストの具体例としては、送信側でＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を計算し、ＥＣＭに入れて伝送する。

【００１６】

メッセージダイジェストの他の具体例としては、ＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋ）、パリティー、ＢＣＨ符号、リード・ソロモン符号などの秘密情報を使用しない誤り検出可能な符号や、鍵を使用しないハッシュ関数を利用し生成したものである。例えば、放送側で演算したＣＲＣをＥＣＭに入れて伝送する。

【００１７】

メッセージダイジェストのもう一つの他の具体例としては、鍵を使用したハッシュ関数やブロック暗号を利用し生成したものである。使用する鍵は放送局と受信機が予め秘密裏に共有化しているものとし、例えばＥＣＭを暗号化する際に使用するワーク鍵は予め秘密裏に共有化しており、また受信機内でもＩＣカードなどのブロック内に安全に管理されており最適である。ワーク鍵以外にも、放送局と受信機が共有化できている鍵であれば良い。ここで利用するメッセージダイジェストは秘密の鍵を利用して生成しているものであり、鍵を知らない者が

5

生成する危険性は低いため、放送側で演算したメッセージダイジェストを暗号化して伝送する必要は必ずしも無く、ＥＣＭ以外の情報として伝送してもよいし、ＥＣＭに入れて伝送してもよい。

【００１８】

図１はメッセージダイジェストの計算に際し鍵を使用しない場合の例であり、鍵を使用する場合には図示しない鍵の管理部からメッセージダイジェスト計算部１０１，１０２にそれぞれ鍵が入力されるものである。この場合の鍵としてＥＣＭの暗号化に使用されるワーク鍵を使用する場合には、暗号部１０５へ与えられる鍵がメッセージダイジェスト計算部１０１，１０２にもそれぞれ入力される。

【００１９】

ＥＣＭ多重部１０３には、前記メッセージダイジェストの他に、映像音声データなどの番組のスクランブルに使用されるＥＣＭが多重される。ＥＣＭ多重部１０３から出力されたＥＣＭは、暗号化部１０５にて暗号化され、多重部１０６に出力される。

【００２０】

なお、暗号化部１０５で暗号化に使用する鍵をワーク鍵と呼び、図示しないＥＭＭの生成および管理部で生成保持し、暗号化部１０５へ供給されるものである。このワーク鍵はセキュリティーの低下を防ぐという目的から、定期的に例えば１ヶ月に１度という更新周期で更新することがあり、更新時には事前に全ての視聴契約者に向けて更新予定の新しいワーク鍵をＥＭＭに入れ送付するようになっている。放送局では新しいワーク鍵の入ったＥＭＭをほぼすべての受信機が受信した頃を見計らってワーク鍵を更新するものである。

【００２１】

また、スクランブル部１０４では映像音声データなどの番組がスクランクブルされ、多重部１６に出力される。このスクランブルに使用される鍵は、ＥＣＭに多重されるスクランブル鍵である。

【００２２】

以上説明したように、デジタルコピー制御記述子およびコンテント利用記述子のメッセージダイジェストは、ＥＣＭに多重された後、暗号化されて受信機まで改ざんされることなく伝送可能となる。

【００２３】

図２は、この発明の放送受信装置の一実施の形態について説明するためのブロック図である。なお、この図２ではＥＭＭの受信部および暗号復号部や、番組配列情報ＳＩ，ＰＳＩを使用しての番組表生成部や番組表の表示部、リモコン入力部などユーザーインターフェース部、などこの発明の説明に直接関係のないブロックは省略してある。

【００２４】

分離部２０１では、受信した放送信号から番組データ、

6

番組配列情報（ＳＩ，ＰＳＩ）、ＥＣＭ、図示しないＥＭＭを分離する。分離された番組配列情報ＳＩ，ＰＳＩは、さらに分離部２０３にて番組情報配列ＳＩ，ＳＰＩの情報の一部であるデジタルコピー制御記述子およびコンテント利用記述子、それにこれ以外の番組配列情報ＳＩ，ＰＳＩに分離される。ここで他の番組配列情報ＳＩ，ＰＳＩは図示しない番組表生成部で番組表に加工され、オンスクリーン表示などでユーザーに提示したり、選局時の情報として受信機の制御に使用するものである。

【００２５】

デジタルコピー制御記述子およびコンテント利用記述子は著作権保護処理部２１４に与えられ、著作権保護処理部２１４では２つの記述子に従い著作権保護がなされるように、受信機の出力信号を制御したり、図示しない蓄積装置において一時的な蓄積が指定時間の間だけできるように制御したりするものである。また、デジタルコピー制御記述子およびコンテント利用記述子はメッセージダイジェスト計算部２０６，２０７にも与えられ、それぞれのメッセージダイジェストを計算する。

【００２６】

なお、図２はメッセージダイジェストの計算に際し鍵を使用しない場合の例であり、鍵を使用する場合には図示しない鍵の管理部からメッセージダイジェスト計算部２０６，２０７に鍵がそれぞれ入力されるものである。この場合の鍵としてＥＣＭの復号化に使用されＥＭＭメモリ２０５に記憶されているワーク鍵を使用する場合には、このワーク鍵がメッセージダイジェスト計算部２０６，２０７にもそれぞれ与えられる。

【００２７】

次に、分離部２０１で分離されたＥＣＭは、復号部２０２で暗号の復号を行い、分離部２０４でメッセージダイジェスト、スクランブル鍵、番組に関する視聴条件情報に分けられる。

【００２８】

分離部２０４で分離された２つの記述子のメッセージダイジェストはそれぞれ比較部２０９，２１０に与えられ、メッセージダイジェスト計算部２０６，２０７でそれぞれ計算されたメッセージダイジェストと比較判定する。判定の結果はそれぞれ著作権保護処理部２１４に与えられる。

【００２９】

分離部２０４で分離されたスクランブル鍵は、スイッチ２１１、スイッチ２１２を経由して復号部２１３に与え、番組の復号が行われる。復号された番組は、図示しないＭＰＥＧ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｃｏｄｉｎｇ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）でコード処理等をされた後、著作権保護部２１４を経由して視聴者に提供される。

【００３０】

分離部２０４で分離された番組に関する視聴条件情報は、視聴可否判定部２０８でＥＭＭメモリ２０５内の個別契約情報と比較判定処理され、視聴可能かどうかの判定を行う。視聴可と判定された場合には、スイッチ２１１をＯＮし、スクランブル鍵の通過を許可する。

【００３１】

著作権保護処理部２１４では比較部２０９，２１０からデジタルコピー制御記述子およびコンテント利用記述子の改ざんの有無が通知され、改ざんがあった場合にスイッチ２１２をＯＦＦし、スクランブルされた番組の暗号を解くスクランブル鍵をデスクランブル部２１３に供給しないこととする。従って、出力信号はスクランブルされたままの番組、もしくは出力信号はミュート状態となる。

【００３２】

ここで、送信側でＭＡＣを計算してＥＣＭに入れて伝送した場合は、受信側で受信したデジタルコピー制御記述子およびコンテント利用記述子からＭＡＣを計算してＥＣＭ内のＭＡＣと比較し改ざんを判定するためのものである。

【００３３】

また、放送側で演算したＣＲＣをＥＣＭに入れて伝送した場合、受信側ではＥＣＭから取り出したＣＲＣと受信した記述子から計算したＣＲＣとを比較し、両者が一致すれば改ざん無し、不一致なら改ざん有りと判断する。なお放送側で演算したＣＲＣは、暗号で保護されたＥＣＭに入れて伝送されるため、このＣＲＣ自体が改ざんされる危険性は低い。

【００３４】

さらに、鍵を使用したハッシュ関数やブロック暗号を利用して生成したものをＥＣＭに入れて伝送した場合、受信機では、伝送された改ざん検出データを利用して、デジタルコピー制御記述子およびコンテント利用記述子の改ざんの検出を行う。もし改ざん有りと検出した場合には、ＥＣＭを使用した視聴可否判定処理によりデスクランブル可（視聴可）であっても、デスクランブル不可とする。

【００３５】

図３は、この発明の放送側の他の実施の形態について説明するためのブロック図である。この実施の形態は、図１と比較して改ざん検出時の制御モード情報をＥＣＭ多重部１３に入力し、ＥＣＭ情報の一部として伝送するところが異なっているのみであるため、以下の説明では、同一の構成部分には同一の符号を付して説明する。

【００３６】

改ざん検出時の制御モード情報とは、受信機でデジタルコピー制御記述子またはコンテント利用記述子の改ざん有りと検出した場合に、受信機が動作すべき制御方法を規定したものである。図４に示すように、改ざん検出時の制御モード情報として３ビットをＡ～Ｃで定義し、ビット１をＡ、ビット２をＢ、ビット３をＣに対応させて指定する。

【００３７】

すなわち、Ａに“１”がたった場合はデスクランブル不可、Ｂに“１”がたった場合は改ざんのあった記述子の無効化（コピー禁止、または一時蓄積不可）、Ｃ“１”がたった場合は、警告のメッセージ表示、Ａ～Ｃのいずれにも“１”がたたない場合は、何もしない、を切り換えるものである。また、ＡからＣに関しては併用可とするように、改ざん検出時の制御モード情報は、例えばビットマップ指定方式とする。

【００３８】

図５を用いてこの発明の放送受信装置の他の実施の形態について説明する。この実施の形態は、図２と比較して図３の送信方法で送信される他の信号とともに多重された改ざん検出時の制御モード情報を、分離部２０４で分離して著作権保護処理部２１４に入力する部分、警告メッセージを表示するためのオンスクリーン表示部２０６の追加した部分が異なっている。また、説明の都合上、ＭＰＥＧデコード処理部２０５も追加している。以下、図２と同一の構成部分には同一の符号を付して説明する。

【００３９】

図５において、分離部２０１では、受信した放送信号から番組データ、番組配列情報（ＳＩ，ＰＳＩ）、ＥＣＭ、図示しないＥＭＭを分離する。分離された番組配列情報ＳＩ，ＰＳＩは、さらに分離部２０３にて番組情報配列ＳＩ，ＳＰＩの情報の一部であるデジタルコピー制御記述子およびコンテント利用記述子、それにこれ以外の番組配列情報ＳＩ，ＰＳＩに分離される。ここで他の番組配列情報ＳＩ，ＰＳＩは図示しない番組表生成部で番組表に加工され、オンスクリーン表示などでユーザーに提示されたり、選局時の情報として受信機の制御に使用するものである。

【００４０】

デジタルコピー制御記述子およびコンテント利用記述子は著作権保護処理部２１４に与えられ、著作権保護処理部２１４では２つの記述子に従い著作権保護がなされるように、受信機の出力信号を制御したり、図示しない蓄積装置において一時的な蓄積が指定時間の間だけできるように制御したりするものである。またデジタルコピー制御記述子およびコンテント利用記述子はメッセージダイジェスト計算部２０６，２０７にも与えられ、それぞれのメッセージダイジェストを計算する。

【００４１】

なお、図５はメッセージダイジェストの計算に際し鍵を使用しない場合の例であり、鍵を使用する場合には図示しない鍵の管理部からメッセージダイジェスト計算部２０６，２０７に鍵がそれぞれ入力されるものである。この場合の鍵としてＥＣＭの復号化に使用されＥＭＭメモ

リ２５に記憶しているワーク鍵を使用する場合には、このワーク鍵がメッセージダイジェスト計算部２０６，２０７にもそれぞれ与えられる。

【００４２】

次に、分離部２０１で分離されたＥＣＭは復号部２０２で復号され、分離部２０４でメッセージダイジェスト、改ざん検出時の制御モード情報、スクランブル鍵、番組に関する視聴条件情報に分けられる。分離部２０４で分離された２つの記述子のメッセージダイジェストは、比較部２０９，２１０にそれぞれ与えられ、メッセージダイジェスト計算部２０６，２０７でそれぞれ計算されたメッセージダイジェストと比較判定する。判定の結果はそれぞれ著作権保護処理部２１４に与えられる。

【００４３】

分離部２０４で分離されたスクランブル鍵は、スイッチ２１１，２１２を経由して番組のデスクランブル部２１３に与えられ、デスクランブルされた番組は、ＭＰＥＧデコード処理部２１５でデコード処理等をされた後、オンスクリーン表示部２１６および著作権保護部２１４を経由して視聴者に提供される。

【００４４】

分離部２０４で分離された番組に関する視聴条件情報は、視聴可否判定部２０８でＥＭＭメモリ２０５内の個別契約情報と比較判定処理され、視聴可能かどうかの判定を行う。判定の結果視聴可と判定した場合には、スイッチ２１１をＯＮし、スクランブル鍵の通過を許可する。

【００４５】

著作権保護処理部２１４では比較部２０９，２１０からデジタルコピー制御記述子およびコンテント利用記述子の改ざんの有無が通知され、改ざんがあった場合には、分離部２０４から入力される改ざん検出時の制御モード情報に従い受信機を制御する。

【００４６】

なお、改ざん検出時の制御モード情報は、図４に示すように、改ざん検出時の制御モード情報として３ビットをＡ～Ｃで定義し、ビット１をＡ、ビット２をＢ、ビット３をＣに対応させて指定する。

【００４７】

すなわち、デスクランブル不可の場合には、著作権保護処理部２１４はスイッチ２１２をＯＦＦし、スクランブル鍵を番組のデスクランブル部２１３に供給しないこととする。従って、出力信号はスクランブルされたままの番組となる。

【００４８】

警告のメッセージ表示の場合には、著作権保護処理部２１４はオンスクリーン表示部２１６に対し警告のメッセージ表示を行うように制御する。なお、警告メッセージは固定的なメッセージとして著作権保護処理部２１４で予め製造時等に記憶しておき、著作権保護処理部２１４

に対しデータ提示しても良いし、番組配列情報ＳＩ，ＰＳＩの一部として放送側から提供されたものを、分離部２０３で分離し使用しても良いものとする。

【００４９】

改ざんのあった記述子の無効化の場合には、著作権保護処理部２１４は改ざんのあった記述子の無効化を行うように動作する。すなわち、デジタルコピー制御記述子に改ざんがあった場合には出力信号をコピー禁止の制御をした上で出力するものである。また、コンテント利用記述子に改ざんがあった場合には、図示しない蓄積装置に対し番組の一時蓄積を不可とする制御を行うものである。

【００５０】

以上説明した例では、メッセージダイジェストをＥＣＭ内で伝送する例であったが、メッセージダイジェストをワーク鍵等の暗号鍵を使用し計算するものとすればＥＣＭ内で伝送する必要はない。その場合には、暗号鍵を管理している管理部、例えば受信機に使用されるＩＣカードなどでデジタルコピー制御記述子もしくはコンテント利用記述子からメッセージダイジェストの計算を行うこととし、暗号鍵が公開されないようにするものとする。

【００５１】

そしてＩＣカードにはＥＣＭを処理し、契約がある場合にはスクランブル鍵が出力される処理とともに、前記メッセージダイジェストの計算結果と、伝送されたメッセージダイジェストの比較を行い、改ざんがあった場合にはＩＣカードから前記スクランブル鍵の出力を行わない等の処理をするものである。

【００５２】

以上説明したように、著作権保護方式に関わるデジタルコピー制御記述子またはコンテント利用記述子の改ざん検出をすることにより、両記述子の改ざんを検出することができ、改ざんがあった場合には視聴不可等の制御をすることで改ざんの抑止することができる。

【００５３】

また、改ざん検出用のメッセージダイジェストは、スクランブル鍵とともにＥＣＭ内で暗号化され伝送されるため、メッセージダイジェスト自体の改ざんがされることなく安全に受信機に伝送されるほか、スクランブル鍵の管理と平行して改ざんの有無を検出するため、改ざんがあった場合には視聴不可等の制御をすることも可能となる。

【００５４】

さらには改ざんが検出された場合の受信機制御の方法を複数種類設け、放送波で制御可能とすることにより、改ざんがあった場合のペナルティーのレベルを切り換えることが可能となる。

【００５５】

【発明の効果】

以上説明したように、この発明によれば、著作権保護用

11

の情報であるデジタルコピー制御記述子およびコンテント利用記述子に改ざんがあるかを検出し、改ざんが検出された場合は視聴不可等の制御を行い、改ざんを抑止することが可能となる。

【図面の簡単な説明】

【図１】この発明の送信側の一実施の形態について説明するためのブロック図。

【図２】この発明の受信側の一実施の形態について説明するためのブロック図。

【図３】この発明の送信側の他の実施の形態について説明するためのブロック図。

【図４】この発明の改ざん検出時の制御内容について説明するための説明図。

【図５】この発明の受信側の他の実施の形態について説明するためのブロック図。

【符号の説明】

12

１０１，１０２，２０６，２０７・・・メッセージダイジェスト計算部

１０３・・・ＥＣＭ多重部

１０４・・・スクランブル部

１０５・・・暗号化部

１０６・・・多重部

２０１，２０３，２０４・・・分離部

２０２・・・復号部

２１３・・・デスクランブル部

２０５・・・ＥＭＭメモリ

２０８・・・視聴可否判定部

２０９，２１０・・・比較部

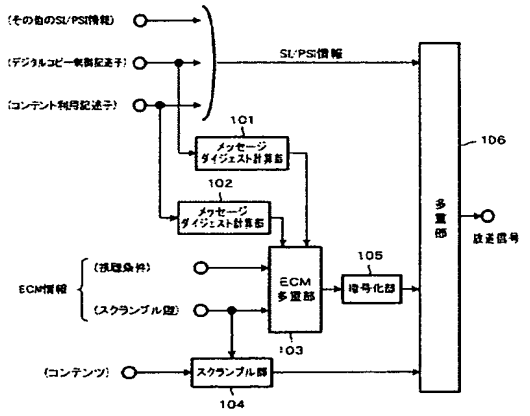
２１１，２１２・・・スイッチ

２１４・・・著作権保護処理部

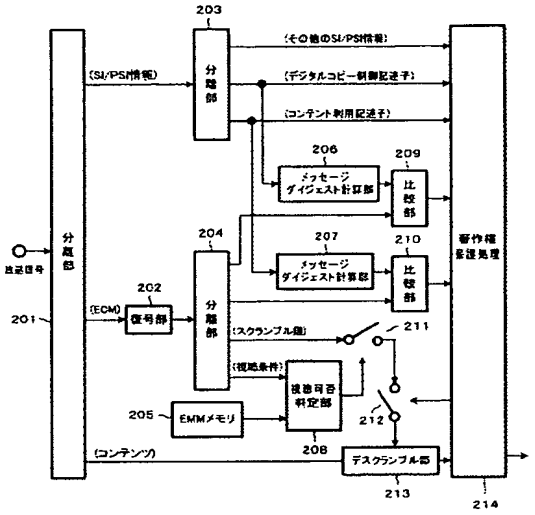
２１５・・・ＭＰＥＧデコード処理部

２１６・・・オンスクリーン表示部

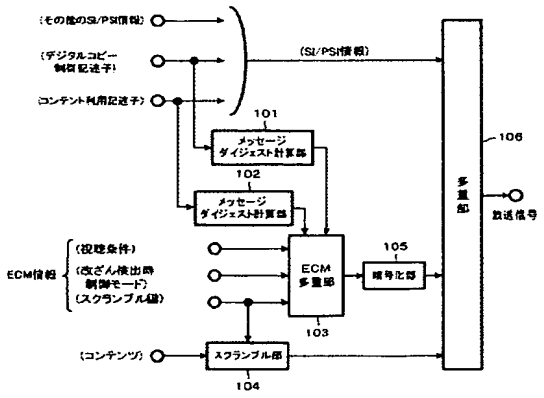
【図１】



【図２】



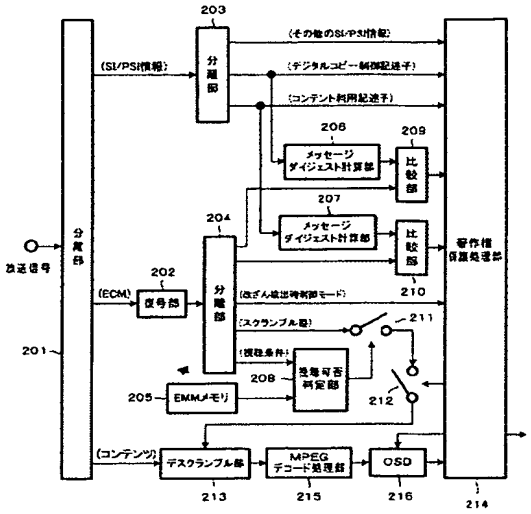
【図３】



【図４】

ビット			改ざん検出時の制御内容
A	B	C	
0	0	0	何もしない
1	0	0	デスクランブル不可
0	1	0	改ざんのあった記述子の無効化（コピー禁止、または一時蓄積不可）
0	0	1	警告のメッセージ表示
1	1	0	デスクランブル不可、改ざんのあった記述子の無効化（コピー禁止、または一時蓄積不可）
1	0	1	デスクランブル不可、警告のメッセージ表示
0	1	1	改ざんのあった記述子の無効化（コピー禁止、または一時蓄積不可）、警告のメッセージ表示
1	1	1	デスクランブル不可、改ざんのあった記述子の無効化（コピー禁止、または一時蓄積不可）、警告のメッセージ表示

【図５】



フロントページの続き

(51) Int. Cl.[7]		F I			テーマコード（参考）
Ｈ０４Ｎ	7/08	Ｈ０４Ｎ	7/08	Ｚ	
Ｈ０４Ｎ	7/081	Ｈ０４Ｎ	7/167	Ｚ	
Ｈ０４Ｎ	7/167	Ｈ０４Ｌ	9/00	６０１Ｂ	

Ｆターム(参考) 5J104 AA08 AA12 AA13 LA01 LA02 LA05 NA02 NA35 PA05
5K028 EE05 KK01 KK03 KK12